THE HON. JOHN C. COUGHENOUR

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

JANE DOE, Individually and on Behalf of All Others Similarly Situated,

Plaintiff,

v.

MICROSOFT CORPORATION, a Washington Corporation; QUALTRICS INTERNATIONAL INC., a Delaware Corporation; and QUALTRICS LLC, a Delaware Limited Liability,

Defendants.

Case No. 2:23-cv-718-JCC

PLAINTIFF'S OPPOSITION TO DEFENDANT MICROSOFT CORPORATION'S MOTION TO DISMISS PLAINTIFF'S COMPLAINT

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

TABLE OF CONTENTS

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

TABLE OF AUTHORITIES

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

I. INTRODUCTION

This privacy action seeks redress for Defendant Microsoft Corporation's unlawful collection of Plaintiff's personal healthcare information while she used her healthcare provider's website. Microsoft intercepts and obtains this data using its tracking software, which collects Plaintiff's medical conditions, immunizations, allergies, search terms, visited URLs, and prescriptions, along with unique user identifiers. Recognizing that health information is some of the most sensitive information there is, federal law prohibits its use and disclosure.

Microsoft moves to dismiss, arguing that Plaintiff consented to the collection of her personal information and that the claims are not adequately pled. But Plaintiff did not consent, and has adequately pled her claims.

First, contrary to Microsoft's claim, Microsoft's misconduct is not disclosed within the healthcare provider's Privacy Statement.[1] The policy does not identify Microsoft or the types of data collected, thus constituting inadequate disclosure.

Second, each of the claims in the Complaint is sufficiently pled. Plaintiff's claims are adequately pled because Plaintiff has a protected property interest in their personal identifiable information, including medical information, and Microsoft improperly and without compensation to Plaintiff, obtained that information. Article III standing has thus been sufficiently alleged. And while not required for all claims, Microsoft obtained Plaintiff's information in a manner that can identify Plaintiff. Microsoft's motion to dismiss must be denied.

---

[1] Microsoft seeks to have the Court take judicial notice of three policies not discussed or referenced in the Complaint as the subject policies are located on public websites. *See* ECF 43 at pg. 1, fn. 1 ("MTD"). The Court should deny the request. Courts may only take judicial notice of adjudicative facts that are 'not subject to reasonable dispute." *U.S. v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003). Facts appropriate for judicial notice can include matters of public record, but not "disputed facts contained in such public records." *Khoja v. Orexigen Therapeutics*, 899 F.3d 989, 999 (9th Cir. 2018). Other facts suitable for judicial notice include "(1) scientific facts: for instance, when does the sun rise or set; (2) matters of geography: for instance, what are the boundaries of state; or (3) matters of political history: for instance, who was president in 1958." *Shahar v. Bowers*, 120 F.3d 211, 214 (11th Cir. 1997). even when a document can be the subject of judicial notice, the scope of judicial notice does not extend to the truth of the content. *See Garner v. Amazon*, 603 F. Supp.3d 985, 993-994 (W.D. Wash. 2022).

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

II. STATEMENT OF FACTS

A. Microsoft's Software Developer Kit

Microsoft offers a variety of computer hardware and software products, and its Search and News Advertising Business segment "is designed to deliver relevant search, native, and display advertising to a global audience." ¶8.[2] One of these products is a software developer kit (the "Microsoft SDK") comprising tracking software that collects a user's internet data through unique user identifiers and cookies. ¶33. These identifiers include the Microsoft Machine Unique Identifier ("MUID"); Windows Live ID ("WLID"), and the user's WLS identifier ("WLS"). *Id.* Each of these identifiers is unique to a specific user, and the WLS includes a user's real name. ¶¶34-36. The SDK also collects and sends to Microsoft identifying information about a user's web browser ("User Agent Data"). ¶37.

B. Microsoft Intercepts and Collects Plaintiff's Personal Information

Plaintiff has been a member of Kaiser Permanente ("Kaiser Member"), a healthcare provider that serves 12.6 million members across 8 states, for at least 10 years and has used the Kaiser Website throughout her membership. ¶¶7, 28. While logged into her account on the Kaiser Website, she has used the search function; accessed immunization and medical records; made appointments; reviewed physician information; reviewed medical conditions; and watched videos. *Id.* Microsoft has intercepted and collected Plaintiff's information during her use of the Kaiser Website. *Id.*

Specifically, the Microsoft SDK intercepts and collects a plethora of user data and content based on a user's browsing activity on the Kaiser Website ("Private Data"), including personally identifiable information ("PII") and protected health information ("PHI"), from Kaiser Members when they use the Kaiser Website without their knowledge or consent. ¶38. The Microsoft SDK intercepts and collects the search terms entered by the user in the Kaiser Website's integrated search bar without regard for their sensitivity (i.e., it takes the most sensitive medical inquiries,

[2] All "¶__" citations are to the Complaint (ECF No. 1, the "Complaint").

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

along with unique user identifiers including MUID, WLID, and WLS. ¶¶39-40. It intercepts and collects the visited URL and webpage title—which divulge the Kaiser Member's medications, medical conditions, immunization, and/or allergies—along with unique user identifiers such as MUID, WLID, and WLS that enable Microsoft to link this sensitive information to a specific user. ¶¶42-43, 45. This interception and collection occurs regardless of whether the user is logged into her Kaiser account, and Microsoft's ability to identify a user is enhanced by the SDK's collection of User Agent Data. ¶¶39, 42,

The SDK collects still more PHI and user identifiers when Kaiser Members are logged into their account and access personal medical data from the Website's personalized subpages. For example, when a Kaiser Member accesses information about her medications, medical conditions, and immunizations from her personalized "Prescription Details," "Health Summary," and "Medical Record" pages, the SDK intercepts and collects the URL (which includes the medication's reference number and name, the name of the condition, the immunization name, and which reveals the user navigated from these private webpages) and unique user identifiers. ¶¶47, 50, 53, 56.

This misconduct enables Microsoft to determine that the specific Kaiser Member is prescribed a medication, suffers from a medical condition or allergy, and/or has received an immunization. *Id.*

C. Plaintiff's Personal Information, Especially Health Information, Is Protected

Patient health care information is protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and regulations promulgated thereunder by the U.S. Department of Health and Human Services. ¶¶14, 17-18. HIPAA provides that individuals' PHI may not be used or disclosed except as specifically permitted or required by the rule. ¶16. Health information is individually identifiable unless there is little risk that a recipient could identify the individual or if identifiers (including URLs, IP addresses, and other unique identifying numbers, characteristics, or code) are removed. ¶19. There is no HIPAA-exception for the Internet or online patient portals. ¶25. Regardless of HIPAA, a patient does not consent to a third-party intercepting

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

and collecting Private Data unless the individual understands that she is authorizing the third party to collect such private medical information. ¶27. To obtain consent, the interception and collection of an individual's medical information must be specifically disclosed. Disclosure that an individual's information is taken, without specific disclosure that medical information is taken does not suffice. *Id.*

D. Plaintiff's PII Has Value

Numerous academic articles confirm that user's personal data has significant economic value. ¶¶88-102. Corporate monetization of user data is nearly ubiquitous, and several large corporations have transformed their models from fee-for-services-provided to monetizing their users' data, including data that is not necessary for the product or service use. ¶92. Revenue from user data pervades a large swath of economic transactions in the modern economy, and fundamental to these revenues is the fact that there is a market for this data. *Id.* Thus, data generated by Kaiser Members has economic value. *Id.* Microsoft intercepted and collected Plaintiff's Private Data without providing anything of value in exchange. ¶103.

There are market exchanges where individual users like Plaintiff can sell or monetize their own data, and there is growing interest in users' medical data. ¶¶94, 99. The value of a single user's data ranges from $15 to more than $40. ¶90. There is also a private market for users' personal information, where an individual's online identity can be sold for $1,200 on the dark web, which is an illegal marketplace. ¶97. De-identified patient data also has value, and experts warn that "clues in anonymized patient dossiers make it possible for outsiders to determine [an individual's] identity." ¶101. Microsoft has accessed Plaintiff's Private Data without permission, and this unauthorized access has diminished the value of that Private Data. ¶104.

III. ARGUMENT

A. Plaintiff Sufficiently Alleges She Was Affected by Microsoft's Conduct

Defendant contends that "Plaintiff fails to allege any facts plausibly showing Microsoft's supposed conduct impacted her in any way." It is unclear from this vague assertion whether Defendant suggests that Plaintiff fails to meet the pleading requirements of Rule 8 of the Federal

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

Rules of Civil Procedure or that Plaintiff has failed to allege an injury-in-fact. It ultimately does not matter since Plaintiff succeeds in doing both.

1. Plaintiff's Allegations Meet the Requirements of Rule 8

To survive a motion to dismiss under Rule 8, "a complaint must contain sufficient factual matter, *accepted as true*, to 'state a claim to relief that is *plausible on its face*.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quotation *omitted*) (emphasis added). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the *reasonable inference* that the defendant is liable for the misconduct alleged." *Id.* (citation *omitted*) (emphasis added). Rule 8 "*does not require 'detailed factual allegations[.]*'" *Id.* (citation omitted) (emphasis added).

Plaintiff's allegations readily meet this standard. In arguing otherwise on the basis that Plaintiff "does not plead the dates she used the Kaiser Website or when Microsoft allegedly 'intercepted and collected' her data (MTD at 16), Defendant ignores Plaintiff's allegations and imposes on Plaintiff a stricter standard than that required by Rule 8.[3] *See Brodsky v. Apple, Inc.*, 445 F. Supp. 3d 110, 135 (N.D. Cal. 2020) ("a failure to plead when any alleged misconduct occurred will not necessarily be fatal under Rule 8.")

Plaintiff alleges that she "has been a Kaiser Member for at least 10 years and has used the Kaiser Website *throughout* her membership" to "use[] the search function; access[] immunization and medical records; ma[k]e appointments; review[] physician information; and watch[] videos" and that Defendant "unlawfully intercepted and collected such data along with her personal identifiers" thereby causing her harm. ¶10. Given that Kaiser is Plaintiff's healthcare provider, with which she has engaged regularly over the past 10 years, it is unreasonable to require Plaintiff to identify each time she used the Kaiser Website and for what purpose. It is sufficient that Plaintiff

[3] Defendant seemingly attempts to impose on Plaintiff a pleading standard more akin to that of Rule 9, which applies to claims sounding in fraud or mistake and requires a party to state the circumstances constituting those claims "with particularity." *See* Fed. R. Civ. P. 9. But none of Plaintiff's claims sound in fraud, and none of her claims are otherwise subject to a heightened pleading standard.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

alleges that she has used the Website "throughout" her membership, meaning that she has used it "during the whole course or period of" her membership. *See Throughout*, Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/throughout (last accessed Aug. 3, 2023). Furthermore, Plaintiff alleges that Defendant collects the at-issue data from Kaiser Members, including her, "when they use the Kaiser Website," including "whenever" they use the Kaiser Website's integrated search bar, navigate to webpages or videos on the Kaiser Website, or log in to their Kaiser Accounts to view their prescriptions, medical conditions, immunization records, and allergies. ¶¶38, 39, 40, 42, 43, 45, 47, 50, 53, 56. When read together, the crux of Plaintiff's allegations is clear: Defendant continuously collected and intercepted Plaintiff's PII and PHI each time she used the Kaiser Website from the time Defendant's SDK was included on the Kaiser Website.[4] Defendant is not left guessing how its wrongful conduct "affected her individually." *See* MTD at 15.

The cases Defendant relies on are inapposite. In *In re Google Assistant Priv. Litig.*, the court held that the plaintiffs' allegations regarding the at-issue recorded conversations were "too vague" because they failed to show, at minimum, that the plaintiffs frequently had oral communications near their respective Google Assistant Enabled Devices under circumstances giving rise to a reasonable expectation of privacy. *See* 457 F. Supp. 3d 797, 816-17 (N.D. Cal. 2020). Similarly, in *Russo v. Microsoft Corp.* the court dismissed the plaintiffs' claims for lack of standing where the plaintiffs only "generically state[d] that Microsoft used and shared 'Plaintiffs' and Class Members'' data" without alleging that they used the at-issue software. *See* 2021 WL 2688850 (N.D. Cal. June 30, 2021). *Martin v. Sephora USA, Inc.* is separately distinguishable because the plaintiff there merely claimed that the purported violation occurred "sometime within the past year." Each of these cases is a significant departure from Plaintiff's allegations detailing how Defendant intercepts Kaiser Member' data and uses it to identify them,

[4] Plaintiff cannot be expected to know when Kaiser included Defendant's SDK on the Kaiser Website. That fact will be learned through discovery.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

and that she has regularly used the Kaiser Website "throughout" her membership over the course of at least 10 years and had her personal data intercepted by Defendant each time.

Finally, since Defendant does not deny that it collected data about Plaintiff's use of the Kaiser Website, it is reasonable to conclude that Defendant is in possession of the information necessary to determine when Plaintiff used the Kaiser Website and when Defendant collected and intercepted the at-issue data.

2. Plaintiff Has Alleged an Injury-in-Fact Resulting from Defendant's Data Collection

To the extent Defendant contends that Plaintiff has not plead an injury in fact and therefore lacks Article III standing, that faulty claim ignores Plaintiff's express allegations in the Complaint.

Plaintiff *repeatedly* alleges that "the unique user identifiers allow Microsoft to link" a Kaiser Member's PII and PHI—search terms, visited webpages, viewed videos, prescriptions, medical conditions, immunization records, and allergies—"to a specific user and *identify the user*," and that "the ability to *identify* the Kaiser Member is enhanced by the SDK's collection of User Agent Data." ¶¶38, 39, 42, 43, 45, 47, 50, 53, 56. It is black letter law that at the pleading stage, Plaintiff's allegations must be taken as true and construed in the light most favorable to her. *See, e.g.*, *In re Facebook Internet Tracking Litigation*, 956 F.3d 589, 597 ("Where standing is raised in connection with a motion to dismiss, the court is to 'accept as true all material allegations of the complaint, and . . . construe the complaint in favor of the complaining party.'") (9th Cir. 2020) (*quotation omitted*). And in any event, Defendant cites to nothing in the Complaint or any other source that contradicts or casts doubt on the plausibility of Plaintiff's allegations.

Additionally, in the Ninth Circuit, the unlawful collection of data impairs a person's privacy rights and confers Article III standing where that data is "personal" or "sensitive." *See, e.g.*, *id.* at 598 (finding standing for common law and statutory privacy claims where Facebook collected plaintiffs' "sensitive" and "personal" browsing histories); *Al-Ahmed v. Twitter, Inc.*, 2023 WL 27356, at *6 (N.D. Cal. Jan. 3, 2023) (finding standing for CIPA claim where plaintiff alleged interception of "private" information including "private messages, direct message, online

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

chats, friend requests, file transfers, file uploads, and file downloads")[5]; *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 784 (N.D. Cal. 2019) ("[D]isclosure of sensitive private information, even without further consequence – gives rise to Article III standing."); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1041 (N.D. Cal. 2014) (explaining that "courts make their decisions regarding whether a plaintiff has stated a legally protectable privacy interest based on the nature of the information at issue" and holding "there can be a legally protected privacy interest or reasonable expectation of privacy in any confidential and sensitive content"); *Byars v. Goodyear Tire & Rubber Co.*, 2023 WL 2996686, at *3 (C.D. Cal. 2023); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034,1049 (N.D. Cal. 2022); *see also TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021) (explaining that "various intangible harms," including "disclosure of private information, and intrusion upon seclusion" are "concrete" injuries); *Norman–Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1271 n.17 (9th Cir. 1998) ("Under California law, a legally recognizable privacy interest arises from the sort of information revealed[.]").

Facebook Tracking is illustrative. There, the plaintiffs had standing to bring their invasion of privacy, intrusion upon seclusion, and CIPA claims based on their allegations that Facebook collected their data "in order to receive and compile their *personally identifiable* browsing history . . . no 'matter how sensitive' or personal users' browsing histories were" and that "by correlating users' browsing history with users' personal Facebook profiles—profiles that could include a user's employment history and political and religious affiliations—Facebook gained a cradle-to-grave profile without users' consent." *See* 956 F.3d at 598-99 (emphasis added). Consistent with *Facebook Tracking,* in a decision issued this month, the Northern District of California held that the privacy harm resulting from the collection and use of private browsing history is a sufficiently concrete injury to confer standing. *See Brown, et al. v. Google LLC*, Case No. 4:20-cv-3664, ECF

[5] As relates to CIPA claims specifically, numerous courts "have held that allegations of violations of Plaintiffs' statutory rights under CIPA, without more, constitute injury in fact." *Osgood v. Main Streat Mktg.*, LLC, 2017 WL 131829, at *7 (S.D. Cal. Jan. 13, 2017) (collecting cases).

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

969, at 9-10 (N.D. Cal. Aug. 7, 2023). Given the recognized privacy interests in data such as employment history and political religious affiliation, the standing principles articulated in *Facebook Tracking* apply with even greater force to Plaintiff, who alleges that Defendant intercepted her PHI and linked it directly to her.

B. Plaintiff States a Claim Under CIPA

"CIPA prohibits any person from using electronic means to 'learn the contents or meaning' of any 'communication' 'without consent' or in an 'unauthorized manner.'" *See id.* 605 (quoting Cal. Pen. Code § 631(a)). Further, CIPA applies nationwide for the reasons described in the UCL section, *infra*.

1. Microsoft Intercepted the Contents of Plaintiff's Communications

Plaintiff adequately alleges that Microsoft intercepted the "contents" of her communications: the Microsoft SDK collects the search terms, visited URLs, prescriptions, medical indications, immunization records, and allergies of Kaiser Members. ¶¶33-59.

In contending otherwise, Microsoft primarily relies on a case holding that "record information" such as the "name, address, and subscriber number or identity of a subscriber or customer" does not constitute "contents" of the communication. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). But Microsoft overlooks that where, as here, the URL contains search terms, the URLs qualify as content. *See In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1083 (N.D. Cal. 2015) ("to the extent the URLs contain a user's search terms," they are "content"). *Zynga* acknowledges this: "Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to a disclosure of the contents of the communication." *Zynga,* 750 F.3d at 1108-09.

Here, when Microsoft collects the visited URLs, it collects the "contents" of the communication. *Facebook Tracking*, 956 F.3d at 605 (URLs that "could divulge a user's personal interests, queries, and habits" is "content"). For prescriptions, the URL "includes the medication's reference number in Kaiser's 'Drug encyclopedia' and sometimes the medication's name." ¶47.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

For medical conditions, the URL "contains the name of the medical condition used for the search query and reveals that the user navigated from her personalized 'Health Summary' subpage within her 'Medical Record' page accessed from her Kaiser Account," thereby revealing that the Kaiser Member is afflicted with the medical condition. ¶50. For immunization records, the URL "contains the name of the immunization used for the search query and reveals that the user navigated from her personalized 'Medical Record' page accessed from her Kaiser Account," thereby revealing that the Kaiser Member has had a particular immunization. ¶53. For allergies, the URL "contains the name of the allergy used for the search query and reveals that the user navigated from her personalized 'Medical Record' page accessed from her Kaiser Account," thereby revealing that the Kaiser Member has a particular allergy. ¶56. Microsoft's own authority recognizes that referrer URLs that reveal a user's entered data, such as medical conditions, qualifies as content. *See* MTD at 10, *citing Katz-Lacabe v. Oracle America, Inc.*, --- F. Supp. 3d ---, 2023 WL 2838118, at *9 (N.D. Cal. Apr. 6, 2023) (citing *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003))

Microsoft also incorrectly claims that Plaintiff's allegations about search terms and other medical information is "general health information that is accessible to the public at large." MTD at 10-11. First, this is indisputably the "content" of the communications. Second, Plaintiff has a reasonable expectation of privacy as to this information; Microsoft not only collected that Plaintiff viewed a particular webpage with health information but intercepted unique user identifiers and User Agent Data enabling Microsoft to link this sensitive information to a specific user. ¶¶33-59. And, at the pleading stage, Plaintiff need not identify the specific mechanism by which Microsoft is able to link the unique identifier to the specific Kaiser Member. *Greenley v. Kochava, Inc.*, 2023 WL 4833466, at *17 (S.D. Cal. July 27, 2023) (SDK collection of users' "personal characteristics" and "search terms" sufficient to allege "contents").

2. Plaintiff Lacked Notice of the Microsoft SDK

In the Ninth Circuit, a consent defense to wiretapping claims is met if the plaintiff assented to online contracts – such as through terms of use or privacy policies – that are both sufficiently conspicuous *and* sufficiently detailed to constitute actual or inquiry notice of the relevant conduct.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1177 (9th Cir. 2014); *Smith v. Facebook, Inc.*, 745 Fed. Appx. 8, 9 (9th Cir. 2018) ("in determining consent, courts consider whether the circumstances, considered as a whole, demonstrate that a reasonable person understood that an action would be carried out so that their acquiescence demonstrates knowing authorization."). The allegations of the Complaint sufficiently refute that Microsoft met this standard *even if* the Court takes judicial notice of the privacy policies as argued by Microsoft.

Microsoft does not cite any provision in the Kaiser Privacy Statement that conspicuously and with sufficient detail discloses that ***Microsoft*** would intercept and collect Kaiser Website users' search terms, visited URLs, and protected health information. Three of the five cited provisions discuss that ***Kaiser*** will collect certain data, but of course, Kaiser is the website operator and medical provider, and by virtue of that relationship has the user's medical data. Thus, a user has little reason to challenge that her own healthcare provider collects "unique identifiers" and "health or medical information." Kaiser is not Microsoft.

The closest the Kaiser Privacy Statement comes to disclosing the alleged interception and collection is the statement that "software development kits (SDKs)" can collect usage data, but that "is not identifiable to you as an individual." MTD at 12. This, however, fails to discuss the collected data with specificity. *Cf. Silver v. Stripe, Inc.*, 2021 WL 3191752, at *4 (N.D. Cal. July 28, 2021) (disclosing that "identifiers, demographic information, commercial information, relevant order information, internet activity, geolocation data, sensory information, and inferences" were collected and tracked by third parties); *Garner v. Amazon.com, Inc.*, 603 F. Supp. 3d 985, 997 (W.D. Wash. 2022) (disclosing that voice assistant stored user voice inputs and used that information to improve services). Moreover, that disclosure explicitly disclaims what Plaintiff alleges—that Microsoft collects Private Data along with unique user identifiers that enable it to identify specific Kaiser Members—thus is inadequate notice. *Brown v. Google, LLC*, 525 F. Supp. 3d 1049, 1066 (N.D. Cal. Dec. 22, 2021) (data collection disclosures inadequate when contradicted by other statements).

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

3. Microsoft Intercepted Protected Communications

Microsoft insists that the first clause of § 631(a) (i.e., interception) applies strictly to "telegraph" or "telephone," not computers as alleged here. MTD at 12-13. However, the Ninth Circuit has already cautioned against restricting privacy statutes to archaic technologies because the "use of cookies to track and compile internet browsing histories provide access to a category of information otherwise unknowable and implicate privacy concerns in a manner different from traditional intrusions as a ride on horseback is different from a flight to the moon." *Facebook Tracking*, 956 F.3d at 603 (cleaned up). That the 1967 statute does not specifically state "computers" does not preclude liability here. Indeed, courts have found an adequate interception claim had been stated against software providers. *See, e.g.*, *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1036-37 (N.D. Cal. 2014) (email scanning technology); *see also In re Meta Pixel Healthcare Litig.*, --- F. Supp. 3d ---, 2022 WL 17869218, at *14-15 (N.D. Cal. Dec. 22, 2022) (computer code to obtain healthcare information).

Microsoft does not (and cannot) challenge that its conduct violates the second clause of § 631(a) (i.e., eavesdropping). *See* MTD at 12-13; *In re Google Inc. Gmail Litig.*, 2013 WL 5423918, at *20 (N.D. Cal. Sept. 26, 2013) ("the limitation of 'telegraphic or telephone' on 'wire, line, cable, or instrument' in the first clause" is not imported to the second clause).

4. Microsoft Acted with Requisite Intent and Satisfies the Device Requirement Under California Penal Code Section 632

Microsoft argues Plaintiff's Complaint fails to allege that Microsoft intended to "capture sensitive or confidential communications for an impermissible purpose." MTD at 12. Not so. The Complaint specifically alleges that Microsoft "intercept[ed] and collect[ed] [Plaintiff's] activity and … private medical data [and that Microsoft] covertly employ[ed] their tracking code such that [Plaintiff had] no indication that [her] web activity is transmitted to [Microsoft]." ¶30. The impermissible purpose is also evident when considering that the information accessed amounts to sensitive consumer health-related information. Clearly, Plaintiff has a right to have such material

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

protected and kept confidential. ¶¶14-25. Such facts more than meet the pleading standard applicable to Plaintiff's CIPA claim.[6]

In arguing that Plaintiff's Section 632 claim fails because "she does not allege Microsoft used any 'electronic amplifying or recording device[s]' to record her information," Microsoft simply ignores the express allegation of the Complaint that it used "receiving servers (where the data is saved and recorded) which are recording devices under CIPA, to eavesdrop upon the confidential communications." ¶141. *See Brown v. Google LLC*, 525 F.Supp.3d 1049, 1064, 1073-74 (N.D. Cal. 2021) (holding CIPA claim adequately pled where Google "automatically collect[ed] and store[d] certain information in server logs"). Indeed, in enacting section 632 as part of the California Invasion of Privacy Act in 1967, the Legislature specifically found that "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Kight v. CashCall, Inc.,* 200 Cal.App.4th 1377, 1388 (2011). The Complaint adequately alleges that Microsoft used such a recording device.

C. Invasion of Privacy and Intrusion Upon Seclusion

Plaintiff plausibly alleges violations of her privacy rights under the common law and the California Constitution. The combined inquiry for both claims considers "(1) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification and other relevant interests." *Hernandez v. Hillsides Inc.*, 47 Cal. 4th 272, 288 (2009). These highly fact-intensive inquiries are best reserved for a jury. *Meta Pixel*, 2022 WL 17869218, at *15.

[6] The Court, respectfully, should strike Microsoft's self-serving argument that its "Advertising Agreement" supports its position. *See* MTD, at 12:24-26. The contents or substance of the Advertising Policy is not capable of being admitted by way of judicial notice. *See, supra*, fn. 1.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

1. Reasonable Expectation of Privacy

A reasonable expectation of privacy exists where defendants gain "unwanted access to data by electronic or other covert means, in violation of the law or social norms." *Facebook Tracking*, 956 F.3d at 601-02. In evaluating whether data collection is actionable due to a reasonable expectation of privacy, courts consider "the amount of data collected, the sensitivity of the data collected, the nature of the data collection, and [defendant's] representations to users." *Calhoun v. Google, LLC*, 526 F. Supp. 3d 605, 621 (N.D. Cal. 2021). Due to this holistic analysis, "courts hesitate to decide the issue at the pleadings stage." *Greenley*, 2023 WL 4833466, at *12.

Courts have concluded that there is a reasonable expectation of privacy over "detailed URL requests, app browsing histories, and search queries." *Rodriguez v. Google LLC*, 2021 WL 2026726, *8 (N.D. Cal. May 21, 2021). Microsoft's challenge that the collected data does not constitute "content" fails. *See* Sec. III.B.1, *supra*. Plaintiff's allegations that Microsoft collects search terms, visited URLs, prescriptions, medications, immunizations, and allergies is sufficiently specific. *Cf.* MTD at 15 (citing *Yahoo Mail*, 7 F. Supp. 3d at 1040 (bare allegation of privacy interest in "email *generally*" is insufficient). And, the Ninth Circuit has already rejected Microsoft's contention that a plaintiff must "identify specific, sensitive information" collected. *Facebook Tracking*, 956 F.3d at 603.

Contrary to Microsoft's claim, this expectation of privacy is reasonable regardless of whether a user is logged into the Kaiser Website. *E.g.*, *In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d 935, 946-47 (N.D. Cal. 2022) (reasonable expectation of privacy over "web browsing histories, device information, and consumer interest data."). "[S]uch information is personal information under California law and parties generally maintain a reasonable expectation [of privacy] in their personal information." *Id.* (citing Cal. Civ. Code § 1798.140). Also, the HHS bulletin cited by Microsoft does not support its position, since it describes how tracking technologies can have access to PHI even when the patient is not logged in.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

2. Highly Offensive Intrusion

Whether the collection of personal information is offensive or serious is a question "best left for a jury." *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1061 (N.D. Cal. 2014). Collection of Plaintiff's activity on her healthcare provider's website is highly offensive. *See, e.g.*, *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) (associating Plaintiff's browsing history with his identity could be "highly offensive breach of norms"). Microsoft speculates that a user may be searching for medical conditions or immunizations "for a friend or family member, or simply out of general curiosity, or perhaps because they work in healthcare"—plainly ignoring Plaintiff's allegations that this medical information is collected from her personalized Medical Record on the Kaiser Website. ¶¶47, 50, 53, 56.

Microsoft argues that the offensiveness of the intrusion requires allegations as to the use of the collected data. MTD at 17-18. Not so. Its cited cases rely on *Fogelstrom v. Lamps Plus, Inc.*, which held that "obtaining plaintiff's address without his knowledge or permission" to send coupons "is not an egregious breach of social norms." 125 Cal. Rptr. 3d 260, 265 (2011); *see also White v. Social Security Admin.*, F. Supp. 3d 1041, 1053 (N.D. Cal. 2015) ("unauthorized photocopies of identity documents" by government official not "highly offensive" absent improper use). However, other courts have recognized that cases which "mechanically applied *Fogelstrom* to invasion of privacy claims" do not explain "why [such] practices were consistent with community notions of privacy as they existed at the time of the decision." *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1079 (N.D. Cal. 2016) (could not find as a matter of law that "surreptitious theft of personal contact information" from smartphones is "routine commercial behavior"). Because the Private Data includes sensitive information such as medical conditions affecting an individual, a reasonable person is likely to find collection of such information to be highly offensive. *Doe v. Regents of Univ. of Cal.*, --- F. Supp. 3d ---, 2023 WL 3316766, at *6 (N.D. Cal. May 8, 2023) ("Personal medical information is understood to be among the most sensitive information that could be collected about a person.").

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

This is a context-specific inquiry, which is why, "[u]nder California law, courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is." *Facebook Consumer Privacy Litig.*, 402 F. Supp. At 797 ("egregious" privacy violation when Facebook shared users' "sensitive information on a widespread basis" with its business partners); *see also Facebook Tracking*, 956 F.3d at 606 (offensiveness of "tracking and collection practices . . . cannot be resolved at the pleading stage").

D. CFAA

Defendant's argument that Plaintiff fails to plead a CFAA claim centers around the mistaken notion that Plaintiff "does not allege that Microsoft accessed her *computer* without her consent." MTD at 27. Defendant overlooks Plaintiff's allegations that Defendant's SDK collects users' internet data "through several unique identifiers *and cookies*," including the MUID cookie. ¶¶ 33, 34.[7] Put simply, Defendant accessed Plaintiff's computer when it installed cookies on it via it's SDK. ¶¶33, 34, 180. By using the cookies it surreptitiously installed on Plaintiff's computer without her consent via its SDK, Defendant was able to intercept Plaintiff's private data, including PII and PHI, while she used the Kaiser Website and identify her by linking that data to her. *See id.*

Even assuming *arguendo* that Plaintiff consented (she did not) to Defendant's accessing her computer—*i.e.*, installing cookies—pursuant to Kaiser's Privacy Statement (MTD at 13-14), Plaintiff separately alleges that Defendant *exceeded* any authority she may have given it by intercepting her private data, including her highly sensitive medical information, and linking it to her. The wording of Kaiser Privacy Statement could not and did not reasonably put Plaintiff on notice that by letting Defendant install cookies on her computer she was also granting Microsoft carte blanche authority to collect her medical information and identity. *See Meta Pixel*, 2022 WL 17869218, *9-10 (holding that plaintiffs did not consent to Meta's collection of their medical

[7] It is widely known that cookies are small blocks of data created by a server while a user is browsing a website and placed on the *user's computer*. *See https://en.wikipedia.org/wiki/HTTP_cookie*.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

information where Meta's policies did not "specifically indicate that Meta may acquire health data obtained from Facebook users' interactions with their medical providers' websites"). CFAA liability attaches for the "unauthorized procurement or alteration of information." *Brodsky*, 445 F.Supp.3d at 128 (N.D. Cal. 2020).

Finally, the CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Plaintiff suffered such damage. *See, e.g.*, ¶¶66-67, 68-70, 71-73, 74-75, 76-78, 79-81, 82-84, 85-87, 88, 103-104, 180. The CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Plaintiff and Class Members have suffered loss of at least $5,000 in the form of retaining a technical expert to investigate Microsoft's surreptitious interception and collection of their data in order to "respond[] to an offense" and to "restor[e] the data . . . to its condition prior to the offense" (i.e., to being in the exclusive possession of the Class and Kaiser).

E. Unjust Enrichment

Defendant's contentions that Plaintiff fails to state a claim for unjust enrichment are meritless.

First, under California law, unjust enrichment *is* an independent cause of action. *Bruton v. Gerber Prods. Co.*, 703 Fed. Appx. 468, 470 (9th Cir. 2017) (recognizing that the California Supreme Court allowed an independent claim for unjust enrichment); *Williams v. Facebook, Inc.*, 384 F.Supp.3d 1043, 1057 (N.D. Cal. 2018). "To allege unjust enrichment as an independent cause of action, a plaintiff must show that the defendant received and unjustly retained a benefit

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

at the plaintiff's expense." *ESG Cap. Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016) (citing *Lectrodryer v. SeoulBank*, 77 Cal.App.4th 723, 726, 91 Cal.Rptr.2d 881 (2000)).[8]

Plaintiff's sufficiently pleads each of these elements by alleging, *inter alia*, that: (i) Defendant "intercepted and collected Plaintiff's and Class Members' Private Data, including PHI and PII, without providing anything of value to Plaintiff and Class Members in exchange for that Private Data" and "without permission," and that the "unauthorized access" "has diminished the value of that Private Data" and "resulted in harm to Plaintiff and Class Members" (¶¶103-104); (ii) Defendant knowingly and willingly benefitted from its collection, interception, and use Plaintiff's data and the "revenues and profits resulting from targeted advertising and other uses of such data" (¶¶ 186-187); (iii) Plaintiff expected that Defendant "would not intercept, collect, and use" her data (¶ 188); and (iv) Defendant "reaped benefits that led to [it] wrongfully receiving profits" through "deliberate violation of Plaintiff, Class Members, and Subclass Members' privacy interests and statutory and constitutional rights" (¶ 189).

Alternatively, "[w]hen a plaintiff alleges unjust enrichment, a court may 'construe the cause of action as a quasi-contract claim seeking restitution." *Astiana v. Hain Celestial Group, Inc*., 783 F.3d 753, 762 (9th Cir. 2015). Plaintiff adequately pleads an unjust enrichment claim as a quasi-contract claim based on the allegations referenced immediately above.

Second, Plaintiff also need not show she lacks an adequate legal remedy at the pleading stage to proceed on her claim for unjust enrichment. It is "clearly established circuit practice allowing plaintiffs to plead in the alternative at the earliest stages of litigation." *See Haas v.*

---

[8] Defendant's contention that Plaintiff "must also plead that "Microsoft's actions directly caused her to expend her own financial resources or caused her data to become less valuable" utterly misstates the law. MTD at 28 (citing *Katz-Lacabe v. Oracle Am., Inc*, 2023 WL 2838118, at *10 (N.D. Cal. April 6, 2023). What *Katz-Lacabe* actually states is that "California law requires disgorgement of unjustly earned profits ***regardless*** of whether a defendant's actions caused a plaintiff to directly expend his or her own financial resources or whether a defendant's actions directly caused the plaintiff's property to become less valuable." *Id.* (citation omitted) (emphasis added). But even if Defendant were right, Plaintiff clears this hurdle, since she pleads that Defendant's unauthorized access to her private data has "diminished the value of that Private Data" and "resulted in harm to Plaintiff." ¶ 104.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

Travelex Ins. Servs. Inc., 555 F. Supp. 3d 970, 980 (C.D. Cal. 2021) (allowing unjust enrichment claim to proceed in the alternative at the pleading stage) (citation omitted). Regardless, Plaintiff adequately pleads that she lacks a legal remedy. ¶¶139, 150, 192.

Third, Plaintiff need not allege, as Defendant claims, "an actionable misrepresentation or omission", since none of Plaintiff's claims sounds in fraud. *See Hammerling*, 2022 WL 17365255, at *12 (N.D. Cal. Dec. 1, 2022) (dismissing unjust enrichment claim where plaintiffs "failed to allege an actionable misrepresentation or omission" "because the Court again finds that Plaintiffs' fraud claims cannot survive a motion to dismiss"). But even if that was a necessary element of Plaintiff's claim, Plaintiff has pled it by alleging that Defendant has covertly and unlawfully collected her PII and PHI without her knowledge or consent. *See, e.g.*, ¶¶30, 32, 67, 105, 188.

Accordingly, Plaintiff's unjust enrichment claim should be allowed to proceed.[9]

F. UCL

1. Plaintiff Has Standing to Bring Her UCL Claim

Defendant acknowledges that Plaintiff alleges that she "lost consideration for provision of access to [her] Private Data" and suffered "diminished value of that data" (¶¶ 104, 204) but argues that Plaintiff lacks standing because "sharing personal information does not constitute lost money or property for UCL standing purposes." Defendant's argument is contrary to the law.

As a threshold matter, "the 'economic injury' required by the UCL is a 'classic form of injury in fact' under Article III." *Brown v. Google LLC*, 2021 WL 6064009, at *17 (N.D. Cal. Dec. 22, 2021). Defendant's attempt to impose a higher standing threshold for UCL claims therefore fails.

Plaintiff suffered a cognizable "economic injury" resulting from Defendant's improper interception and use of her personal information. *Kwikset Corp. v. Sup. Ct.*, 51 Cal.4th 310, 321 (2011). Plaintiff has alleged the existence of a market for her data (¶¶88–102) and that the value

[9] Plaintiff's unjust enrichment claim should be allowed to proceed under Washington law to the extent the Court is hesitant to apply California law.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

of her data—which is property under the California Consumer Privacy Act (*see* Cal. Civ. Code § 1798.140(v)(1))—was diminished due to Defendants' conduct (¶¶104, 204). Such allegations suffice to confer standing under the UCL. *See Brown*, 2021 WL 6064009, at *16 (finding standing under similar circumstances) (collecting cases); *Calhoun*, 526 F.Supp.3d at 636 ("plaintiffs who suffered a loss of their personal information suffered economic injury"); *Guy v. Convergent Outsourcing, Inc.*, 2023 WL 4637318, at *10 (W.D. Wash. July 20, 2023) ("Plaintiffs have pointed out that their PII has lost value by virtue of the breach. This is an economic injury sufficient under the UCL.").

Defendant's reliance on *Campbell v. Facebook, Inc*., 77 F. Supp. 3d 836 (N.D. Cal. 2014), *Gonzales v. Uber Technologies*, 305 F. Supp. 3d 1078 (N.D. Cal. 2018), and *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705 (N.D. Cal. 2011) is inapt. Those decisions predate *Facebook Tracking*, which held that plaintiffs have suffered an economic injury for standing purposes from the improper collection of their personal information. 956 F.3d at 600–01. Since *Facebook Tracking*, many courts have found similar allegations regarding the loss of users' personal information, for which there is a market, enough to confer UCL standing.[10] *E.g., Klein v. Facebook, Inc.*, 580 F.Supp.3d 743, 803 (N.D. Cal. 2022) ("by providing [defendant] with their information and attention," plaintiffs had alleged they "lost money or property") (citation omitted); *Griffey v. Magellan Health Inc.*, 2022 WL 1811165, *10 (D. Ariz.) (same).

2. Plaintiff States Claims Under the UCL's "Unlawful" and "Unfair" Prongs

Unlawful. Defendant agrees that the "unlawful" prong of the UCL prohibits conduct forbidden by law. MTD at 29. Plaintiff adequately pleads unlawful conduct based on statutory and common law violations. ¶¶127-191, 206-215; *see also Calhoun*, 526 F. Supp. 3d at 636

[10] Defendant's reliance on *Katz-Lacabe* is also of no moment because even assuming *arguendo* that case is correct that "the 'mere misappropriation of personal information' does not establish compensable damages," Plaintiff has "alleged a specific monetary or economic loss." *See* 2023 WL 2838118, at *8.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

(upholding UCL claim where plaintiffs pled CIPA and statutory larceny claims); *Brown*, 2021 WL 6064009, *14 (similar).

Unfair. Plaintiffs' allegations pass all three tests recognized in California courts. *In re Zoom Video Commc'ns Inc. Privacy Litig.*, 525 F.Supp. 3d 1017, 1047 (N.D. Cal. 2021) (describing each test in detail). Plaintiffs meet: (i) the "immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers" test because Defendants caused Plaintiff to suffer loss and diminution of the value of her private data (¶¶104, 204), and because surreptitious privacy invasions and taking of personal information is unethical and unscrupulous (¶202); (ii) the tethering test, because the conduct violated privacy, data, and consumer protections established by constitutional and statutory authority, including Article I of the California Constitution, CIPA, CFAA, Larceny, and Conversion (¶¶127-191, 206-215); and (3) the balancing test, because the harm was significant without a countervailing benefit, particularly since Defendant's interception of Plaintiff's and Kaiser Members' PII and PHI is unnecessary for the provision of medical services (¶ 31). *See In re Zoom Video Commc'ns Inc. Privacy Litig.*, 525 F.Supp. 3d at 1047.

3. The UCL Applies to Kaiser Members Not Residing in California

Defendant's contention that the UCL does not apply extraterritorially fares no better than its other arguments. The UCL "may be invoked by out-of-state parties when they are harmed by wrongful conduct occurring in California." *Effinger v. Ancient Organics LLC*, 2023 WL 2214168, at *7 (N.D. Cal. Feb. 24, 2023) (quoting *In re iPhone 4S Consumer Litig.*, 2013 WL 3829653, at *7 (N.D. Cal. July 23, 2013)). Whether the UCL may be applied to interstate plaintiffs involves a two-step process:

> First, the plaintiff bears the onus to demonstrate the application of California law comports with due process. This involves establishing "sufficient contacts" between the alleged misconduct and the state. Second, the onus then shifts to the defendant to show that foreign law, rather than California law, should apply to these claims.

Id. (quoting *Arroyo v. TP-Link USA Corp.*, 2015 WL 5698752, at *3 (N.D. Cal. Sept. 29, 2015). Plaintiff (a California resident) adequately pleads that Defendant's wrongful conduct occurred in

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

California, because Defendant's data-intercepting SDK is employed by Kaiser, an entity headquartered in California, and because Defendant has offices and conducts substantial business in California. ¶¶28, 30, 124. The logical inferences from those allegations are that: (i) the Kaiser Website, which employs Defendant's SDK, is hosted on servers in California, and Kaiser Members' private data is therefore unlawfully intercepted in California; and (ii) Defendant has servers in California that through which the SDK intercepts and stores Kaiser Members' private data.[11] Furthermore, "Defendant has failed to show (or even argue) that another forum's law should apply," which is fatal to its argument. *Effinger*, 2023 WL 2214168, at *7; *McKinney v. Corsair Gaming, Inc.*, 2022 WL 2820097, at *13 (N.D. Cal. July 19, 2022) ("Corsair has not provided a sufficient description of other state laws to meet its burden of showing that Plaintiffs lack standing to bring claims under these other states' laws."). In any event, the applicability of the UCL to Kaiser Members who do not reside in California is an issue to be decided at a later stage in this litigation. *See Effinger*, 2023 WL 2214168, at *7 (allowing UCL claim to proceed past MTD but noting that "proving that California law is appropriate for the Nationwide lass may ultimately be difficult"); *McKinney*, 2022 WL 2820097, at *13 (allowing UCL claim to proceed past MTD but allowing defendant to argue against extraterritoriality "at a later date").

G. Statutory Larceny

Statutory larceny prohibits knowingly receiving stolen property or property obtained "in any manner constituting theft." Cal. Penal Code § 496. The property interest "need not be one that was considered property at common law and, of course, need not be tangible." *G.S. Rasmussen & Assocs., Inc. v. Kalitta Flying Serv., Inc.*, 958 F.2d 896, 902 (9th Cir. 1992); *see also Voris v. Lampert*, 7 Cal. 5th 1141, 1151 (2019). Microsoft's claim that personal information does not constitute "property" is contradicted by many cases holding that people have a property interest in their personal information. *See, e.g.*, *Calhoun*, 526 F. Supp. 3d at 635 (noting this argument

[11] Plaintiff should be given the opportunity to prove these inferences through discovery. To the extent the Court deems these inferences unsupported by Plaintiff's allegations, Plaintiff should be allowed to amend her Complaint to plead them expressly.

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

"ignores this Court's other rulings both before and after *Low v. LinkedIn*"); *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 798-99 (N.D. Cal. 2011) (similar); *see also CTC Real Estate Servs. v. Lepe*, 44 Cal. Rptr. 3d 823, 825 (2006) ("A person's identifying information is a valuable asset.").

Microsoft's assertion that it did not obtain the data in a manner constituting theft fails. First, the Kaiser Privacy Statement does not sufficiently disclose the nature of the interception and collection. *See* Sec.III.B.2, *supra*. Second, Section 496(a) extends to property that has been obtained in *any manner* constituting theft." Cal. Penal Code § 496. This includes misrepresentation. *Grouse River Outfitters, Ltd. v. Oracle Corp.,* 848 Fed. Appx. 238, 242 (9th Cir. 2021) (software provider knew that certain funds were obtained in a manner constituting theft where provider misrepresented nature of software products). Plaintiff alleges that she lacked notice of the collection of her personal information and, in fact, the Kaiser Privacy Statement misrepresents that third parties will not be able to identify individuals by their data. This misrepresentation suffices. Further, the statutory larceny claim applies nationwide for the reasons described in the UCL section, *supra*.

H. Conversion

"Conversion is the wrongful exercise of dominion over the personal property of another." *Taylor v. Forte Hotels Int'l*, 1 Cal. Rptr. 2d 189, 192 (1991). Conversion deals with control over personal property. *See id.*; *Facebook Tracking*, 956 F.3d at 598 (A "right to privacy encompasses the individual's control of information concerning his or her person.") (cleaned up). To plead conversion under California law, pleadings must allege "(1) the plaintiff's ownership or right to possession of personal property; (2) the defendant's disposition of the property in a manner that is inconsistent with the plaintiff's property rights; and (3) resulting damages." *Fremont Indem. Co. v. Fremont Gen. Corp*., 148 Cal. App. 4th 97, 119 (2007). Here, Plaintiff alleged a right to possess control over her personal information (¶¶32-87, 175–77, 205, 227, 238, 247, 255, 378); Microsoft's interference with her right to control her property and/or the outright taking of it (¶¶22-27, 30, 32, 33-40, 211-215, 209); and resulting damages (¶88-104, 146, 105). Thus, Plaintiffs

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

adequately state a claim for conversion. Microsoft's only challenge is that personal information is not property, which fails for the same reasons as for the statutory larceny claim.

I. Punitive Damages

"[A] request for punitive damages is not a 'claim' and is not the proper subject of a motion to dismiss under Fed. R. Civ. P. 12(b)(6)." *Shimy v. Wright Med. Tech., Inc.*, 2014 WL 3694140, at *4 (C.D. Cal. July 23, 2014).

IV. CONCLUSION

For the foregoing reasons, Microsoft's motion to dismiss must be denied.[12]

DATED this 14th day of August 2023.

SUMMIT LAW GROUP, PLLC

I certify that this memorandum contains 8,352 words in compliance with the Local Civil Rules.

By *s/ Alexander A. Baehr*

Alexander A. Baehr, WSBA No. 25320
Diana Siri Breaux, WSBA No. 46112
315 Fifth Avenue S., Suite 1000
Seattle, WA 98104
Telephone: (206) 676-7000
Email: alexb@summitlaw.com
dianab@summitlaw.com

BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW PC

Ekwan E. Rhow *(Admitted pro hac vice)*
Marc E. Masters *(Admitted pro hac vice)*
Barr Benyamin *(Admitted pro hac vice)*
1875 Century Park East, 23rd Floor
Los Angeles, CA 90067
Telephone: (310) 201-2100
Email: erhow@birdmarella.com
mmasters@birdmarella.com
bbenyamin@birdmarella.com

[12] To the extent the Court finds the Complaint's allegations not supporting Plaintiff's Claims, Plaintiff requests leave pursuant to F. R. Civ. P. 15(a) to amend.

GLANCY PRONGAY & MURRAY LLP

Jonathan Rotter *(Admitted pro hac vice)*
Kara M. Wolke *(Admitted pro hac vice)*
Pavithra Rajesh *(Admitted pro hac vice)*
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160
Email: jrotter@glancylaw.com
kwolke@glancylaw.com
prajesh@glancylaw.com

Counsel for Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on this day I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the following:

Gregory L. Watts, WSBA #43995
Tyre L. Tindall, WSBA #56357
WILSON SONSINI GOODRICH & ROSATI, P.C.
701 Fifth Avenue, Suite 5100
Seattle, WA 98104-7036
Email: gwatts@wsgr.com; ttindall@wsgr.com

Anthony J Weibell *(Admitted pro hac vice)*
WILSON SONSINI GOODRICH & ROSATI, P.C.
650 Page Mill Road
Palo Alto, CA 94304
Email: aweibell@wsgr.com

Sophia M. Mancall-Bitel *(Admitted pro hac vice)*
WILSON SONSINI GOODRICH & ROSATI, P.C.
1900 Avenue of the Stars, 28th Floor
Los Angeles, CA 90067
Email: smancallbitel@wsgr.com

Attorneys for Defendants Qualtrics International Inc. and Qualtrics, LLC

Patricia A. Eakes, WSBA #18888
MORGAN, LEWIS & BOCKIUS LLP
1301 Second Avenue, Suite 2800
Seattle, WA 98101
Email: patty.eakes@morganlewis.com

Kathryn Deal (*Admitted pro hac vice*)
MORGAN LEWIS & BOCKIUS LLP
1701 Market Street
Philadelphia, PA 19103
Email: kathryn.deal@morganlewis.com

Phillip J. Wiese *(Admitted pro hac vice)*
MORGAN LEWIS & BOCKIUS LLP
One Market, Spear Street Tower
San Francisco, CA 94105
Email: phillip.wiese@morganlewis.com

Attorneys for Defendant Microsoft Corporation

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001

DATED this 14th day of August 2023.

s/ Karen M. Lang
Karen M. Lang – Legal Assistant
Summit Law Group, PLLC
karenl@summitlaw.com

SUMMIT LAW GROUP, PLLC
315 FIFTH AVENUE SOUTH, SUITE 1000
SEATTLE, WASHINGTON 98104-2682
Telephone (206) 676-7000
Fax (206) 676-7001